

09/355953

PCT/JP38/00512

日 本 国 特 許 庁

25.02.98

PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1997年 2月13日

REC'D 17 APR 1998

WIPO

PCT

出 願 番 号

Application Number:

平成 9年特許願第028859号

出 願 人

Applicant (s):

ローム株式会社

PRIORITY DOCUMENT

1998年 4月 3日

特許庁長官
Commissioner,
Patent Office

荒井寿光



出証番号 出証特平10-3024708

【書類名】 特許願

【整理番号】 PR700054

【提出日】 平成 9年 2月13日

【あて先】 特許庁長官 殿

【国際特許分類】 G06K 19/00

【発明の名称】 可搬性を有する度数記憶部材およびその運用方法

【請求項の数】 8

【発明者】

【住所又は居所】 京都府京都市右京区西院溝崎町2-1番地 ローム株式会社
社内

【氏名】 疋田 純一

【発明者】

【住所又は居所】 京都府京都市右京区西院溝崎町2-1番地 ローム株式会社
社内

【氏名】 生藤 義弘

【発明者】

【住所又は居所】 京都府京都市右京区西院溝崎町2-1番地 ローム株式会社
社内

【氏名】 田口 治生

【特許出願人】

【識別番号】 000116024

【氏名又は名称】 ローム株式会社

【代表者】 佐藤 研一郎

【代理人】

【識別番号】 100092956

【弁理士】

【氏名又は名称】 古谷 栄男

【電話番号】 06-368-2160

【選任した代理人】

【識別番号】 100101018

【弁理士】

【氏名又は名称】 松下 正

【電話番号】 06-368-2160

【選任した代理人】

【識別番号】 100101546

【弁理士】

【氏名又は名称】 眞島 宏明

【電話番号】 06-368-2160

【手数料の表示】

【予納台帳番号】 004891

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9201113

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 可搬性を有する度数記憶部材およびその運用方法

【特許請求の範囲】

【請求項1】

金銭に対応する度数を記憶する可搬性を有する度数記憶部材であって、
外部から与えられた読み出し命令に基づいて、前記記憶されている度数を読み出して、外部から与えられた度数変更命令に基づいて、前記記憶されている度数を変更する度数記憶部材において、
前記度数の度数変更のうち増加方向への度数変更を回路構成的に禁止したこと
を特徴とする可搬性を有する度数記憶部材。

【請求項2】

請求項1の可搬性を有する度数記憶部材において、さらに、
前記度数記憶部材に予め度数追加書換え用情報を記憶しておき、この度数追加書換え用情報と一致する情報が与えられた場合には、前記回路構成を切換え、前記度数の増加方向への変更を可能としたこと、
を特徴とする可搬性を有する度数記憶部材。

【請求項3】

可搬性を有する度数記憶部材であって、
金銭に対応する度数を記憶する記憶手段であって、書込データを保持可能なデータ保持部を前記度数個数分有する度数記憶手段、
前記度数記憶部材の外部から与えられた読み出し命令に基づいて、前記度数記憶手段に記憶されている度数を読み出す読み出し手段、
前記度数記憶部材の外部から与えられた度数変更命令に基づいて、前記度数記憶手段の前記各データ保持部を書込データを保持する書込み状態から書込データを保持しない非書込状態にだけ変更可能な度数変更手段、
を備えたことを特徴とする可搬性を有する度数記憶部材。

【請求項4】

請求項3の可搬性を有する度数記憶部材において、

度数追加書換え用情報を記憶する度数追加書換え用情報記憶手段、
与えられた情報と前記度数追加書換え用情報とを照合する照合手段、
を備え、

前記度数変更手段は、前記各データ保持部を前記書込み状態から前記非書込状態に変更可能なだけでなく、さらに、前記照合手段の照合結果に基づいて、前記各データ保持部を前記非書込み状態から前記書込状態にも変更可能であること、
を特徴とする可搬性を有する度数記憶部材。

【請求項5】

可搬性を有する度数記憶部材に金銭に対応する度を記憶しておき、外部から与えられた読み出し命令に基づいて前記度数記憶部材に記憶された度を読み出すとともに、外部から与えられた度数変更命令に基づき前記度を変更する度数記憶部材の運用方法であって、

前記度の度数変更のうち増加方向への度数変更を回路構成的に禁止したこと、
を特徴とする可搬性を有する度数記憶部材の運用方法。

【請求項6】

請求項5の可搬性を有する度数記憶部材の運用方法において、さらに、
前記度数記憶部材に予め度数追加書換え用情報を記憶しておき、この度数追加書換え用情報と一致する情報が与えられた場合には、前記回路構成を切換え、前記度の増加方向への変更を可能としたこと、
を特徴とする可搬性を有する度数記憶部材の運用方法。

【請求項7】

可搬性を有する度数記憶部材に金銭に対応する度を記憶しておき、外部から与えられた読み出し命令に基づいて前記度数記憶部材に記憶された度を読み出すとともに、外部から与えられた度数変更命令に基づき前記度を変更する度数記憶部材の運用方法であって、

前記度数記憶部材は、前記度に対応する個数分データ保持部を有しており、
前記各データ保持部は、書込データが保持された書込み状態から、各データ保持部に書込データが保持されていない非書込状態にだけ、前記度の変更が可能で

あること、

を特徴とする可搬性を有する度数記憶部材の運用方法。

【請求項 8】

請求項 7 の可搬性を有する度数記憶部材の運用方法において、

前記度数記憶部材に予め度数追加書換え用情報を記憶させておき、

この度数追加書換え用情報と一致する情報が与えられた場合には、前記各データ保持部を前記書込み状態から前記非書込状態に変更可能なだけでなく、さらに、前記照合手段の照合結果に基づいて、前記各データ保持部を前記非書込み状態から前記書込状態にも変更可能としたこと、

を特徴とする可搬性を有する度数記憶部材の運用方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、度数記憶部材に関するものであり、特に、その機密性の向上に関する。

【0002】

【従来技術】

スキー場のリフトや鉄道の自動改札、荷物の自動仕分け等に、ICカードを用いたデータ通信システムが提案されている。

【0003】

図12に、ICカードを用いたデータ通信システムのうち、非接触式ICカードを用いた通信システムの構成を示す。このシステムは、質問器40（たとえば、スキー場のリフトのゲート内に搭載される）と非接触ICカード20によって構成される。

【0004】

質問器40は、制御部48の制御により、発振回路49からの高周波搬送波をアンテナ41から送り出している。質問器40に対して非接触ICカード20が接近すると、この高周波搬送波が非接触ICカード20のアンテナ23によって受信される。電源生成回路28は、受信した高周波を直流電力に変換して、他の

回路部分に供給する。このようにして、質問器40に近づくと、非接触ICカード20が動作可能となる。

【0005】

また、質問器40から非接触ICカード20に対する情報伝達は、前記高周波搬送波を変復調回路33において復調することにより行なわれる。制御部35は、復調された情報に基づき、メモリ37の内容の変更や情報返信等の必要な処理を行う。

【0006】

一方、非接触ICカード20から質問器40に対しての情報伝達も行われる。非接触ICカード20側には、発振回路が設けられていないので、次の様にして、情報送信が行なわれる。質問器40の側から無変調の高周波搬送波を送り出しておき、非接触ICカード20側にて、変復調回路33により、共振回路22のインピーダンスを変化させる。質問器40は、このインピーダンス変化を、自己側の共振回路42のインピーダンス変化として、変復調回路46により検出して復調する。制御部48は、復調された情報を得て、必要な処理を行う。

【0007】

非接触ICカード20が質問器40から遠ざかると、電力供給が無くなるので、非接触ICカード20の動作は停止する。なお、メモリ37は不揮発性メモリであるので、電力供給が無くなっても、記憶された情報は保持される。

【0008】

以上のような非接触ICカード20のメモリ37に所定の度数を記憶させておき、使用度数に応じてメモリ37のデータを変更することにより、プリペイドカードとして用いることができる。

【0009】

なお、質問器とICカードとの間の通信データは暗号化される。これによって、一旦使用済みのICカードの内容が無断変更されることを防止できる。

【0010】

【発明が解決しようとする課題】

しかしながら、このような従来のICカードを用いた通信システムは、次のよ

うな問題点があった。上記のように、通信データを暗号化しても、その暗号アルゴリズムが解読されると、結局、データ変造が可能となる。したがって、暗号化のみではシステムの機密性を確保することが困難である。

【0011】

特に、質問器を不特定多数の場所に配置するような場合、例えば、公衆電話等においては、質問器が内蔵された電話機を盗まれ、質問器とICカード間でやり取りされる命令を解析されるおそれもある。

【0012】

この発明は、上記のような問題点を解決し、不正使用が困難な可搬性を有する度数記憶部材およびその運用方法を提供することを目的とする。

【0013】

【課題を解決するための手段】

請求項1の可搬性を有する度数記憶部材においては、前記度数の度数変更のうち増加方向への度数変更を回路構成的に禁止したことを特徴とする。

【0014】

請求項2の可搬性を有する度数記憶部材においては、さらに、前記度数記憶部材に予め度数追加書換え用情報を記憶しておき、この度数追加書換え用情報と一致する情報が与えられた場合には、前記回路構成を切換え、前記度数の増加方向への変更を可能としたことを特徴とする。

【0015】

請求項3の可搬性を有する度数記憶部材においては、

金銭に対応する度数を記憶する記憶手段であって、書込データを保持可能なデータ保持部を前記度数個数分有する度数記憶手段、

前記度数記憶部材の外部から与えられた読み出し命令に基づいて、前記度数記憶手段に記憶されている度数を読み出す読み出し手段、

前記度数記憶部材の外部から与えられた度数変更命令に基づいて、前記度数記憶手段の前記各データ保持部を書込データを保持する書込み状態から書込データを保持しない非書込状態にだけ変更可能な度数変更手段、

を備えたことを特徴とする。

【0016】

請求項4の可搬性を有する度数記憶部材においては、
 度数追加書換え用情報を記憶する度数追加書換え用情報記憶手段、
 与えられた情報と前記度数追加書換え用情報とを照合する照合手段、
 を備え、

前記度数変更手段は、前記各データ保持部を前記書込み状態から前記非書込状態に変更可能なだけでなく、さらに、前記照合手段の照合結果に基づいて、前記各データ保持部を前記非書込状態から前記書込状態にも変更可能であること、
 を特徴とする。

【0017】

請求項5の可搬性を有する度数記憶部材の運用方法においては、前記度数の度数変更のうち増加方向への度数変更を回路構成的に禁止したことを特徴とする。

【0018】

請求項6の可搬性を有する度数記憶部材の運用方法においては、前記度数記憶部材に予め度数追加書換え用情報を記憶しておき、この度数追加書換え用情報と一致する情報が与えられた場合には、前記回路構成を切換え、前記度数の増加方向への変更を可能としたことを特徴とする。

【0019】

請求項7の可搬性を有する度数記憶部材の運用方法においては、前記度数記憶部材は、前記度数に対応する個数分データ保持部を有しており、前記各データ保持部は、書込データが保持された書込み状態から、各データ保持部に書込データが保持されていない非書込状態にだけ、前記度数の変更が可能であることを特徴とする。

【0020】

請求項8の可搬性を有する度数記憶部材の運用方法においては、前記度数記憶部材に予め度数追加書換え用情報を記憶させておき、この度数追加書換え用情報と一致する情報が与えられた場合には、前記各データ保持部を前記書込み状態から前記非書込状態に変更可能なだけでなく、さらに、前記照合手段の照合結果に基づいて、前記各データ保持部を前記非書込状態から前記書込状態にも変更可

能としたことを特徴とする。

【0021】

以下、特許請求の範囲に記載した用語と、実施形態との対応について説明する。度数記憶手段は実施形態においては、度数エリア51が該当する。読み出し手段は、主制御部69、アドレスデコーダ65、読み出し変更回路61が該当する。度数変更手段は、主制御部69、アドレスデコーダ65、読み出し変更回路61が該当する。度数追加書換え用情報記憶手段は、機密データエリア53が該当する。照合手段は、暗号照合部63が該当する。

【0022】

また、本明細書において、回路構成的に禁止するとは特定な回路構成を採用することにより、ある処理ができなくすることをいう。すなわち、論理回路または電気回路のように物理的にこれを禁止することをいう。

【0023】

【発明の効果】

請求項1、請求項5の可搬性を有する度数記憶部材またはその運用方法においては、前記度数の度数変更のうち増加方向への度数変更を回路構成的に禁止されている。したがって、度数を増加させるデータ変更を確実に防止することができる。これにより、不正使用が困難な度数記憶部材を提供することができる。

【0024】

請求項2、請求項6の可搬性を有する度数記憶部材またはその運用方法においては、予め記憶した度数追加書換え用情報と一致する情報が与えられた場合には、前記回路構成を切換え、前記度数の増加方向への変更ができる。したがって、必要な場合にのみ、増加方向への度数変更を防止することができる。

【0025】

請求項3、請求項7の可搬性を有する度数記憶部材またはその運用方法においては、前記度数に対応する個数分データ保持部を有しており、前記各データ保持部は、書込データが保持された書込み状態から、各データ保持部に書込データが保持されていない非書込状態にだけ、前記度数の変更が可能である。したがって、度数を増加させるデータ変更を確実に防止することができる。

【0026】

請求項4、請求項8の可搬性を有する度数記憶部材またはその運用方法においては、前記度数記憶部材に予め度数追加書換え用情報を記憶させておき、この度数追加書換え用情報と一致する情報が与えられた場合には、前記各データ保持部を前記書込み状態から前記非書込状態に変更可能なだけでなく、さらに、前記照合手段の照合結果に基づいて、前記各データ保持部を前記非書込み状態から前記書込状態にも変更可能である。したがって、予め記憶させた度数追加書換え用情報と一致する情報が与えられた場合にだけ、前記度数の変更が可能である。これにより、度数を増加させるデータ変更を確実に防止することができる。

【0027】

【発明の実施の形態】

[1. ICカードの機能ブロックについて]

図面を用いて、本発明にかかる度数記憶部材1について説明する。度数記憶部材1は、可搬性を有し、度数記憶手段3、読み出し手段5、度数変更手段7、度数追加書換え用情報記憶手段13、および照合手段11を備えている。

【0028】

度数記憶手段3は、金銭に対応する度数を記憶する記憶手段であって、書込データを保持可能なデータ保持部を前記度数個数分有する。読み出し手段5は、度数記憶部材の外部から与えられた読み出し命令に基づいて、度数記憶手段3に記憶されている度数を読み出す。度数変更手段7は、度数記憶部材の外部から与えられた度数変更命令に基づいて、度数記憶手段3の前記各データ保持部を書込データを保持する書込み状態から書込データを保持しない非書込状態にだけ変更できる。

【0029】

また、度数追加書換え用情報記憶手段13は、度数追加書換え用情報を記憶する。照合手段11は、与えられた情報と前記度数追加書換え用情報とを照合する。度数変更手段7は、前記各データ保持部を前記書込み状態から前記非書込状態に変更可能なだけでなく、さらに、照合手段11の照合結果に基づいて、前記各データ保持部を前記非書込み状態から前記書込状態にも変更できる。

【0030】

したがって、度数を増加させるデータ変更を確実に防止できるとともに、予め記憶させた度数追加書換え用情報と一致する情報が与えられた場合にだけ、前記度数の変更が可能である。

【0031】

[2. ICカードの具体的構成について]

つぎに、本願発明を非接触式ICカードに適用した場合について図2を用いて説明する。

【0032】

非接触式ICカード10は、全体構成としては、従来と同様、アンテナ24、共振回路22、電源生成回路25、変復調回路33、制御部60、およびメモリ50が筐体11に収納されている。なお、筐体11への収納方法、電源の供給方法およびデータの送受信方法については、従来と同様であるので説明は省略する。

【0033】

図2に示す制御部60およびメモリ部50の詳細を、図3に示す。メモリ部50は、度数エリア51、設定情報エリア52、機密データエリア53および機密データエリア54を有する。度数エリア51は、度数を記憶するエリアであり、設定情報エリア52は設定情報を記憶するエリアである。機密データエリア53は、ICカード運用者の暗号を記憶する機密データエリアである。機密データエリア54は、ICカード製造者の機密データを記憶するエリアである。

【0034】

度数エリア51は図3に示すように、128バイト（1024ビット）のデータが記憶可能である。設定情報エリア52は32バイト、機密データエリア53は3バイト、機密データエリア54は3バイトのデータが記憶可能である。

【0035】

[2.1)メモリ部50]

メモリ部50のメモリ構造について、図4、図5を用いて説明する。本実施形態においては、不揮発性メモリとしてEEPROMを採用した。メモリ50は図

4に示すようなセルC11がマトリックス状に配置されている（図示せず）。

【0036】

セルC11のデータを変更する場合（データ書込：データ「0」を保持させること、データ消去：データ「1」を保持させること）、データを読み出す場合の、ビットラインBL、選択ラインSL、ワードラインWLに印加する電圧を図5に示す。

【0037】

メモリセルC11を書込状態とする（データ「0」を保持させる）場合には、ビットラインBLに20(V)を、選択ラインSLに0(V)を、ワードラインWLに20(V)を印加し、ラインAGを開状態とする。これにより、セルC11のフローティングゲートに電子が注入され、データ「0」が保持される状態となる。

【0038】

メモリセルC11を消去状態とする（データ「1」を保持させる）場合には、データ「0」を保持させるのと逆方向の電圧を印加すればよい。すなわち、ビットラインBLに0(V)を、選択ラインSLに20(V)を、ワードラインWLに20(V)を印加し、ラインAGを開状態（または0(V)）とする。これにより、セルC11のフローティングゲートから電子が放出され、データ「1」が保持される状態となる。

【0039】

メモリセルC11の情報を読み出す場合には、選択ラインSLに5(V)を印加し、ワードラインWLに20(V)を、かつビットラインBLにセンスアンプ（図示せず）を接続する。メモリセルC11がデータ「0」または「1」のいずれを記憶しているかで、センスアンプにおける検出結果が変わる。これにより、メモリセルC11にデータ「1」またはデータ「0」が保持されているかを知ることができる。

【0040】

このように、度数エリア51の各メモリセルは、データ「0」またはデータ「1」を記憶しており、各々がデータ保持部を構成する。また、度数エリア51は予め設定された度数に対応する個数分メモリセルを有する。すなわち、度数が1

000度数であれば1000ビット分のメモリセルを有する。

【0041】

設定情報エリア52、機密データエリア53、機密データエリア54については従来と同様、通常のビット長でデータを保持するようにしている。

【0042】

[2.2)制御部60]

つぎに、制御部60について図3を用いて説明する。制御部60は、主制御部69、アドレスデコーダ65、メモリエリア選択検知回路67、暗号照合部63および読み出し変更回路61を有する。

【0043】

主制御部69は、変復調回路33から与えられたデータに基づきアドレスを指定し、アドレスデコーダ65にアドレスを与える。さらに、読み出し変更回路61に対し、読み出し、書込、消去の何れかの命令を与える。また、暗号照合部63に対し、照合対象となる暗号を与える。アドレスデコーダ65によって選択されたアドレスはメモリエリア選択検知回路67によって検知され、メモリエリア選択検知回路67は、暗号照合部63および読み出し変更回路61に選択アドレスを与える。

【0044】

[2.2.1)読み出し変更回路61]

読み出し変更回路61は、主制御部69から与えられる信号に応じて、図5に示す読み出し電圧、書き込み電圧、消去電圧、または後述する動作禁止電圧をメモリ部50に与える。

【0045】

読み出し変更回路61について、図6を用いて説明する。読み出し変更回路61は、選択アドレス特定端子Ts1～Ts3、モード端子Te、モード端子Tfを有する。選択アドレス特定端子Ts1～Ts3には、いずれのエリアが選択されているかを示す信号がメモリエリア選択検知回路67から与えられる。具体的には、度数エリア51が選択されている場合には、選択アドレス特定端子Ts1には電圧「High」が与えられ、設定情報エリア52が選択されている場合に

は、選択アドレス特定端子Ts2には電圧「High」が与えられる。機密データエリア53が選択されている場合には、選択アドレス特定端子Ts3には電圧「High」が与えられる。

【0046】

また、モード端子Te、モード端子Tfには、暗号照合部63から信号が与えられる。本実施形態においては、読み出し変更回路61は、2つのモード端子に印加される電圧に応じて、以下の3つのモードが切換えられる。

【0047】

モード端子Teに電圧「Low」が、モード端子Tfに電圧「Low」が与えられた状態が、モード「0, 0」である。

【0048】

また、モード端子Teに電圧「Low」が、モード端子Tfに電圧「High」が与えられた状態がモード「0, 1」である。

【0049】

また、モード端子Teに電圧「High」が、モード端子Tfに電圧「Low」が与えられた状態がモード「1, 0」である。

【0050】

読み出し変更回路61は、後述するように、選択アドレス特定端子Te1～Te3、モード端子Te、モード端子Tfに与えられている電圧に応じて、動作禁止電圧をメモリ50の各エリアに印加する。

【0051】

各モードにおいて、読み出し変更回路61が印加可能な電圧について説明する。モード「0, 0」においては、選択アドレス特定端子Te1～Te3によって特定される選択アドレスが度数エリア51および設定情報エリア52である場合には、図5に示す書込電圧を出力可能である。しかし、消去電圧については出力できない。

【0052】

モード「1, 0」においては、選択アドレス特定端子Te1～Te3によって特定される選択アドレスが度数エリア51または設定情報エリア52である場合

には、図5に示す書込電圧および消去電圧を出力できる。しかし、選択アドレス特定端子T e 1～T e 3によって特定される選択アドレスが、機密データエリア53、54である場合には、図5に示す書込電圧または消去電圧を出力できない。すなわち、図5に示す書き込みおよび消去については、度数エリア51、設定情報エリア52のみ可能となる。

【0053】

モード「1, 0」においては、選択アドレス特定端子T e 1～T e 3によって特定される選択アドレスが、度数エリア51、設定情報エリア52または機密データエリア53である場合には、図5に示す消去電圧を出力できる。しかし、選択アドレスが機密データエリア54である場合には、消去電圧を出力できない。また、書込電圧については、いずれのエリアについても出力できない。

【0054】

なお、機密データエリア53、機密データエリア54のデータ線は、図3に示すように暗号照合部63に接続されている。したがって、読み出された暗号が主制御部69に与えられることがなく、外部に機密データエリア53および機密データエリア54に記憶された暗号が読み出されることを防止できる。

【0055】

[2.2.2)暗号照合部63]

暗号照合部63は、メモリエリア選択検知回路67から検知信号が与えられると動作可能状態となり、機密データエリア53または機密データエリア54に記憶された暗号と主制御部69から与えられた暗号が一致するか否かを判断する。両者が一致する場合には、読み出し変更回路61のモード端子T e, T fへ電圧「High」を与える。

【0056】

図7を用いて暗号照合部63の詳細について説明する。暗号照合部63は、比較器71、比較器73、データ変換回路75を有する。比較器73は、機密データエリア54に記憶されたICカード製造者用暗号と一致する暗号が主制御部69から与えられた場合に、モード端子T fへ電圧「High」を与える。

【0057】

また、比較器71はデータ変換回路75から与えられたデータおよび機密データエリア53より与えられたデータを合体させた暗号と一致する暗号が主制御部69から与えられた場合に、モード端子Teへ電圧「High」を与える。

【0058】

例えば、機密データエリア54に暗号「10100000」が記憶されており、ICカード運用者が自己の暗号として「1010」を機密データエリア53に記憶させた場合、次の様にして照合が行なわれる。機密データエリア54の暗号「10100000」をデータ変換回路75が変換する。変換結果が「01011111」である場合は、比較器71には、機密データエリア53に記憶されたICカード運用者の暗号「1010」の後に、「01011111」が付加された暗号「101001011111」が与えられる。そして、主制御部69から与えられた照合対象の入力データが、前記暗号「101001011111」と一致するか否かを判断する。

【0059】

なお、比較器71が、主制御部69から与えられたデータから、データ変換回路75からのデータを取り除いて、機密データエリア53に記憶された暗号と比較するようにしてもよい。

【0060】

また、本実施形態においては、ICカード運用者は、ICカード製造者から機密データエリア54の暗号をデータ変換回路75が変換したデータを得て、これを自己の暗号に付加して、照合すべき暗号として主制御部69に与えるようにする必要がある。

【0061】

このように、本実施形態においては、機密データエリア54の暗号をデータ変換して、機密データエリア53の暗号に付加して、主制御部69から与えられた照合対象暗号データと比較するようにしている。したがって、ICカード製造者がICカード運用者毎に異なる暗号を機密データエリア53に記憶させておくことにより、たまたま2つのICカード運用者が同じ暗号を機密データエリア53

に記憶させた場合でも、間違って他方のICカード運用者のICカードを消去することはできないこととなる。

【0062】

なお、いずれの比較器にて照合をするかについては、メモリエリア選択検知回路67から与えられる信号によって決定される。すなわち、検知したエリアが機密データエリア54である場合には比較器73に、機密データエリア53である場合には比較器51および比較器73に、照合処理を可能とする信号が与えられる。

【0063】

[3. ICカードの処理について]

つぎに、図8～図11を用いてデータの読み出し、書き込み、消去、暗号照合の処理について説明する。なお、初期状態では、読み出し変更回路61のモード端子Te、Tfにはそれぞれ電圧「Low」が与えられている。

【0064】

つぎに、主制御部69は、変復調回路33から与えられた命令が読み出し命令か、残度数削除命令か、データ変更命令か、初期化命令かを判断する（ステップST3）。

【0065】

[3.1 読み出し処理]

与えられた命令が読み出し命令である場合には、度数エリア51全部のアドレスを選択する（ステップST5）。そして、読み出し信号を出力する（ステップST7）。これにより、度数エリア51の全データが読み出され、主制御部69に与えられる。主制御部69は与えられたデータのうち、データ「1」が保持されているビットの個数をカウントし、一時記憶する（ステップST9）。つぎに、設定情報エリア52全部のアドレスを選択する（ステップST11）。そして、読み出し変更回路61へ読み出し信号を出力する（ステップST13）。これにより、設定情報エリア52に記憶された設定情報エリアが主制御部69に与えられる。主制御部69はこれを一時記憶する（ステップST15）。主制御部69は、変復調回路33へ一時記憶したデータを出力する（ステップST17）。

これにより外部に度数エリア51に記憶された残度数および設定情報エリア52に記憶された設定情報を出力することができる。

【0066】

[3.2 度数削除処理]

つぎに、ステップST3にて残度数削除命令が与えられた場合について説明する。この場合、主制御部69は、ステップST9にて一時記憶した残度数を読み出す（ステップST19）。そして、データ「1」が保持されている先頭のメモリセルのアドレスを選択する（ステップST21）。主制御部69は、読み出し変更回路61へ書き込み信号（データ「0」を保持させる信号）を与える（ステップST23）。

【0067】

読み出し変更回路61は、この書き込み信号を受けて、図6に示す選択アドレス特定端子およびモード端子に与えられている電圧に応じて、書き込み電圧を印加できる状態であるかどうかを判断する。この場合、選択アドレスは度数エリア51であり、モード端子は各々ステップST1にて「0, 0」となっているので、書き込み可能であると判断し、図5に示す書き込み電圧を出力する（ステップST24）。

【0068】

つぎに、主制御部69はステップST9にて一時記憶した残度数をデクリメントする（ステップST25）。そして、残度数削除処理が終了したメッセージを変復調回路33へ出力する（ステップST27）。これにより、残度数を削除する命令が与えられた場合に、度数エリア51に記憶された度を指定された分だけ減方向に変更することができる。このようにして、予め度数エリア51に記憶された度を読み出し、または度数削除命令に応じて度を減らす方向にデータを変更することができる。

【0069】

[3.3 データ変更処理]

つぎにステップST3にて、データ変更命令が与えられた場合について説明する。データ変更命令は、度数エリア51または設定情報エリア52のデータを変

更する命令であり、機密データエリアに記憶された暗号と照合する照合命令を含む。

【0070】

この場合、主制御部69は機密データエリア53、54のアドレスを選択する（図9ステップST51）。つぎに、暗号照合部63へ検証対象データを出力する（ステップST53）。主制御部69は読み出し変更回路61へ読み出し信号を出力する（ステップST55）。これにより、読み出し変更回路61は読み出し電圧を印加する。暗号照合部63は、機密データエリア53、54から読み出された暗号と、主制御部69から与えられた検証対象データとの照合を行なう（ステップST57）。

【0071】

具体的には既に説明したように、機密データエリア54の記憶された暗号がデータ変換回路75（図7参照）に与えられる。データ変換回路75は所定の規則に基づいてこの暗号を変換し、変換結果を比較器71に与える。また、比較器71には機密データエリア53に記憶されている暗号が与えられる。比較器71はデータ変換回路75から与えられたデータおよび機密データエリア53より与えられたデータを合体させ、入力された検証対象データと一致するか否かを判断する。一致した場合には、比較器71は読み出し変更回路61に対しモード端子Teに電圧「High」を与える。これにより、読み出し変更回路61は、モード「0, 1」となる（図10ステップST61）。

【0072】

つぎに、主制御部69は、度数エリア51および設定情報エリア52の全アドレスを選択する（ステップST63）。つぎに、読み出し変更回路61に消去信号を出力する（ステップST65）。ここで、読み出し変更回路61については、モード「0, 1」であり、かつ選択アドレスが度数エリア51および設定情報エリア52であるので、消去電圧を出力可能である。したがって、読み出し変更回路61は消去電圧を印加する（ステップST66）。かかる消去電圧が与えられると、度数エリア51および設定情報エリア52の全てのビットに「1」が保持される。

【0073】

つぎに、主制御部69は、度数エリア51、設定情報エリア52のうち、必要なビットのみ選択する（ステップST67）。例えば、設定情報エリアに消去日時等を再度書込む必要がある。この様な場合に、データ「0」を保持するビットを選択する。

【0074】

主制御部69は、読み出し変更回路61へ書き込み信号を出力する（ステップST69）。読み出し変更回路61は書込電圧を印加する（ステップST70）。これにより、選択されたビットのみデータ「0」が保持される。そして、主制御部69は、終了メッセージを変復調回路33へ与える（ステップST71）。

【0075】

なお、図9ステップST59にて与えられた検証対象データが不一致である場合には、主制御部69は、度数エリア51および設定情報エリア52の全アドレスを選択する（図10ステップST73）。つぎに、読み出し変更回路61に消去信号を出力する（ステップST75）。読み出し変更回路61は、現在のモードが、モード「0, 0」であるので、消去電圧を出力せずに動作禁止電圧を出力する（ステップST77）。したがって、度数エリア51および設定情報エリア52の内容は変化しない。

【0076】

なお、本実施形態においては、動作禁止電圧として、ラインAGを接地電位とするとともに、他のラインについては開状態とした。

【0077】

つぎに、主制御部69は、度数エリア51、設定情報エリア52のうち、必要なビットのみ選択する（ステップST79）。主制御部69は、読み出し変更回路61へ書き込み信号を出力する（ステップST81）。ここで、現在のモードが「0, 0」で、選択アドレスが度数エリア51および設定情報エリア52であるので、読み出し変更回路61は書込電圧を出力せずに動作禁止電圧を出力する（ステップST83）。したがって、度数エリア51および設定情報エリア52の内容は変化しない。そして、主制御部69は再書き込みができなかった旨をメ

ッセージ出力する（ステップST73）。

【0078】

このように、暗号不一致の場合には、主制御部69から、読み出し変更回路61に対して消去信号および書き込み信号を出力しても、読み出し変更回路61は書き込み電圧および消去電圧を印加しない。

【0079】

このようにして、予めICカード運用者が入力した暗号に、ICカード製造者から与えられたデータと、一致する暗号が与えられた場合にだけ、度数エリア51および設定情報エリア52のデータを変更することができる。したがって、機密性の高いICカードを提供することができる。

【0080】

[3.4 初期化处理]

つぎに、図8ステップST3にて、初期化命令が与えられた場合について、図11を用いて説明する。初期化命令とは、機密データエリア54以外の度数エリア51、設定情報エリア52、機密データエリア53のデータを全て「1」とする命令をいい、ICカード製造者が行なうものである。

【0081】

この場合、主制御部69は、機密データエリア54のアドレスを選択するとともに（ステップST31）、暗号照合部63へ検証対象データを出力する（ステップST32）。主制御部69は、読み出し変更回路61へ読み出し信号を出力する（ステップST33）。読み出し変更回路61は、読み出し電圧を印加する（ステップST34）。暗号照合部63にて暗号が照合される（ステップST35）。この場合は、機密データエリア54に記憶されたデータが比較器73に与えられ、比較器73は主制御部69より与えられた検証対象データと機密データエリア54に記憶された暗号が一致するか否かを判断する（ステップST36）。

【0082】

図10ステップST36にて、照合結果が一致すると判断した場合には、暗号照合部63は、読み出し変更回路61のモード端子Tfに電圧「High」を与

える（ステップST37）。これにより、読み出し変更回路61はモード「1，0」となる。

【0083】

つぎに、主制御部69は、度数エリア51、設定情報エリア52、機密データエリア53の全アドレスを選択する（ステップST38）。そして、読み出し変更回路61へ消去信号を出力する（ステップST39）。ここで、読み出し変更回路61のモードは、モード「1，0」であるので、読み出し変更回路61は消去電圧を印加する（ステップST41）。これにより、度数エリア51、設定情報エリア52、機密データエリア53の全データが初期化される。主制御部69は終了メッセージを変復調回路33へ出力する（ステップST42）。

【0084】

なお、図11ステップST36にて、照合不一致の場合には、読み出し変更回路61のモード端子Tfへ電圧「High」が与えられない。したがって、読み出し変更回路61はモード「0，0」のままである。主制御部69は、度数エリア51、設定情報エリア52、機密データエリア53の全アドレスを選択する（ステップST43）。そして、読み出し変更回路61へ消去信号を出力する（ステップST44）。ここで、読み出し変更回路61のモードは、モード「0，0」であり、選択アドレスが度数エリア51、設定情報エリア52、機密データエリア53であるので、読み出し変更回路61は動作禁止電圧を印加する（ステップST45）。すなわち、度数エリア51、設定情報エリア52、機密データエリア53の全データは初期化されない。主制御部69は初期化不能メッセージを変復調回路33へ出力する（ステップST46）。

【0085】

このように、初期化命令が与えられた場合でも、機密データエリア54に記憶された暗号と一致する検証対象データが与えられた場合にだけ、初期化を行なうことができる。

【0086】

[3.5 暗号記憶処理]

本実施形態においては、機密データエリア53にICカード運用者が暗号を記

憶するために、機密データエリア53のデータが初期化された後、1回に限り機密データエリア53のデータを変更可能としている。すなわち、初期化後、主制御部69に対して機密データエリア53のデータを変更するデータ変更命令が与えられた場合には、主制御部69は1回に限りこれを認め、機密データエリア53に所定の暗号を記憶することができる。具体的には、図10ステップST61からステップST70の処理を行なうことによって可能となる。

【0087】

なお、主制御部69は、機密データエリア53のデータが変更されたかどうかを記憶しており、機密データエリア53のデータを変更する命令が再度与えられた場合には、これを無視する。

【0088】

[4. 他の実施形態]

なお、本実施形態においては非接触のICカードに適用した場合について説明したが、接触式のICカードのについても同様に適用することができる。

【0089】

なお、主制御部69についてはCPUを用いて構成するようにしてもよく、また一部または全部をロジック回路で構成してもよい。読み出し変更回路61、暗号照合部63、メモリエリア選択検知回路67等についても同様である。

【0090】

本実施形態においては、度数エリア51にメモリセルを度数に対応する個数分設定しておき、度数エリア51をモード「0, 0」である場合には、メモリセルにデータ「1」が保持された書き込み状態から、書き込みデータ「1」が保持されていない未書き込み状態にだけデータ変更を可能としている。これにより、ICカードの偽造をより確実に防止することができる。

【0091】

また、通常の読み出し装置においては、度数エリア51のデータを減らす方向にのみ変更する命令しかICカード側に提供しないので、いわゆる”なりすまし”による被害も防止することができる。

【0092】

なお、メモリ50の構成については上記構成に限定されることなく、例えば、度数エリア51および設定情報エリア52を1つのメモリとし、機密データエリア53、機密データエリア54を別のメモリで構成するようにしてもよい。

【0093】

また、機密データエリア53、機密データエリア54と2段階の暗号を設ける必要はなく、何れか一方であってもよい。

【0094】

なお、本実施形態においてはEEPROMをメモリ部50に用いた場合について説明したが、データを変更できるものであれば、どのようなものでもよく、例えば、フラッシュメモリ、強誘電体メモリ等であってもよい。

【0095】

また、電氣的にデータを書き込むだけでなく、光学的等の手段でデータを書き込めるものであっても、書き込みおよび消去の切替えを行なえるものであれば同様に適用することができる。

【0096】

なお、本実施形態においては、暗号照合部からの照合結果が不一致である場合には、暗号照合部63から読み出し変更回路61のモード端子TeおよびTfは、各々「Low」のままである。したがって、読み出し変更回路61は、メモリ部50に対して動作禁止電圧を与えるだけであるので、データが変造されるおそれがない。

【0097】

さらに、度数エリア51のデータを消去しようという信号が与えられた場合には、度数エリア51および設定情報エリア52の全ビットにデータ「0」を保持させるようにし、機密データエリア54の暗号が入れられない限り、再使用ができないようにしてもよい。

【0098】

なお、本実施形態においては暗号照合部63からの一致信号が与えられた場合にだけ、読み出し変更回路61のモード端子Te、Tfに電圧「High」を与

えるようにし、読み出し変更回路61にて主制御部69からのデータ変更信号を無視するようにしたが、主制御部69に対し照合不一致信号を与え、これに基づき、主制御部69がデータ変更ができないと判断し、読み出し変更回路61にデータ変更信号を出力しないようにしてもよい。そして、その旨メッセージ表示するようにしてもよい。

【0099】

また、本実施形態においては、動作禁止電圧として、ラインAGを接地電位とするとともに、他のラインについては開状態としたが、要するに、書き込みまたは消去がされないような電圧であればどのような様なものであってもよく、例えば、書き込みを禁止するにはビットラインBLに0(V)を印加してもよく、消去を禁止するには選択ラインSLに0(V)を印加するようにしてもよい。

【0100】

なお、本実施形態においては、データ「1」が書込まれている状態を書込状態、データ「0」が書込まれている状態を非書込状態、すなわち、データ「1」を書込データとしたが、データ「0」が書込まれている状態を書込状態、すなわち、データ「0」を書込データとしてもよい。

【0101】

また、本実施形態においては、フローティングゲートに電子が注入された状態をデータ「0」が保持された状態としたが、フローティングゲートから電子が引抜かれた状態をデータ「0」が保持された状態としてもよい。

【0102】

なお、本実施形態においては、初期状態でデータ「1」を保持させておき、度数を減らす場合には、対応するビットにデータ「0」を保持させるようにしたが、逆に、初期状態ではデータ「0」を保持させておき、度数を減らす場合には、対応するビットにデータ「1」を保持させるようにしてもよい。

【0103】

また、本実施形態においては、通常は、モード端子Te、Tfへ電圧「Low」を与えて、度数エリア51の度数を減らす方向にのみ書換え可能とするとともに、モード端子Te、Tfへ電圧「High」が与えられると、消去することを

可能としているが、逆に、通常はモード端子T_e、T_fへ電圧「High」が与えておき、モード端子T_e、T_fへ電圧「Low」が与えられると、消去可能となるようにしてもよい。

【0104】

なお、本実施形態においては、動作禁止電圧として、ラインAGを接地電位とするとともに、他のラインについては開状態とした。しかし、前記ラインAGを接地電位とするようにしてもよい。

【図面の簡単な説明】

【図1】

本発明にかかる度数記憶部材1の機能ブロック図を示す図である。

【図2】

本発明にかかるICカード10の構成の概略を示す図である。

【図3】

図2における制御部60およびメモリ部50の詳細を示す図である。

【図4】

メモリ部50のメモリ構造を示す模式図である。

【図5】

読み出し、書き込み、消去および動作禁止電圧の一例を示す図である。

【図6】

読み出し変更回路61、暗号照合部63、メモリエリア選択検知回路67の相関関係を説明するための図である。

【図7】

暗号照合部63の詳細を示す図である。

【図8】

ICカード10における動作を説明するフローチャートである。

【図9】

ICカード10における動作を説明するフローチャートである。

【図10】

ICカード10における動作を説明するフローチャートである。

【図11】

ICカード10における動作を説明するフローチャートである。

【図12】

従来のICカード20およびその質問器40を示す図である。

【符号の説明】

- 50 メモリ部
- 51 度数エリア
- 52 設定情報エリア
- 53 機密データエリア
- 54 機密データエリア
- 61 読み出し変更回路
- 63 暗号照合部
- 65 アドレスデコーダ
- 67 メモリエリア選択検知回路
- 69 主制御部

特許出願人 ローム株式会社

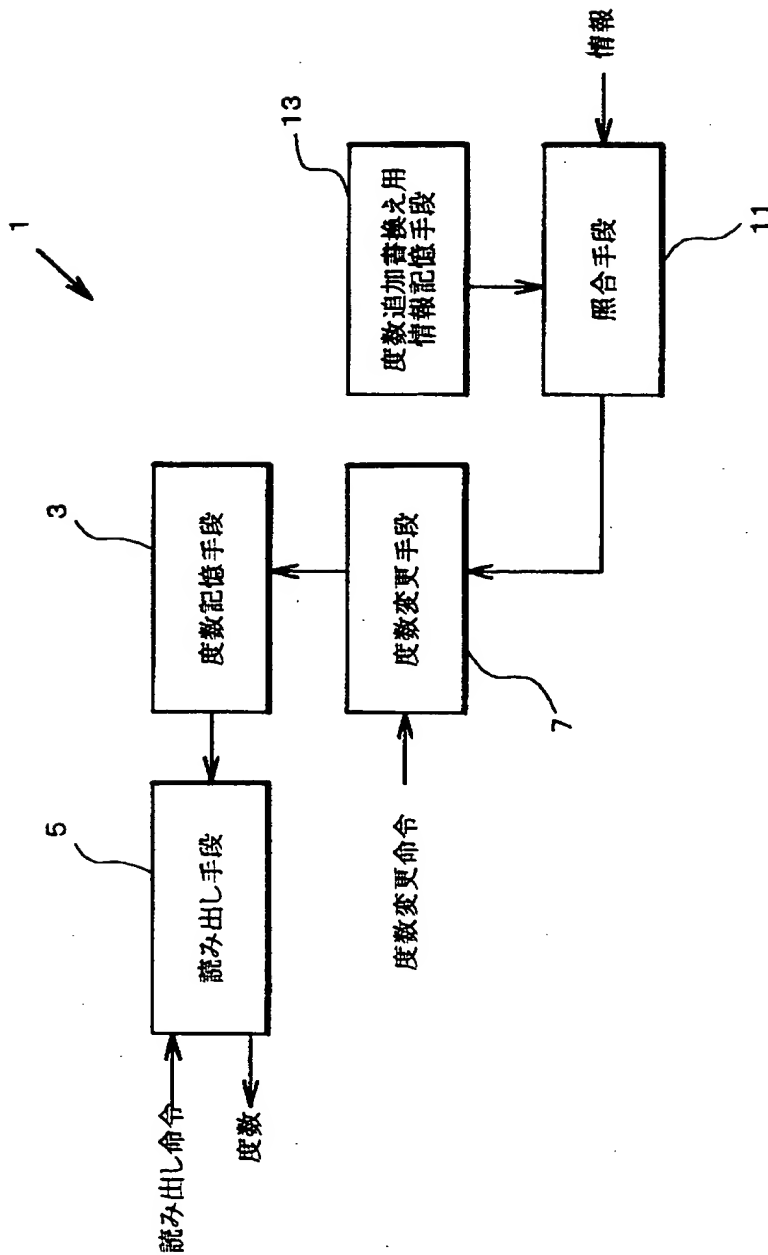
出願人代理人 弁理士 古谷栄男

出願人代理人 弁理士 松下 正

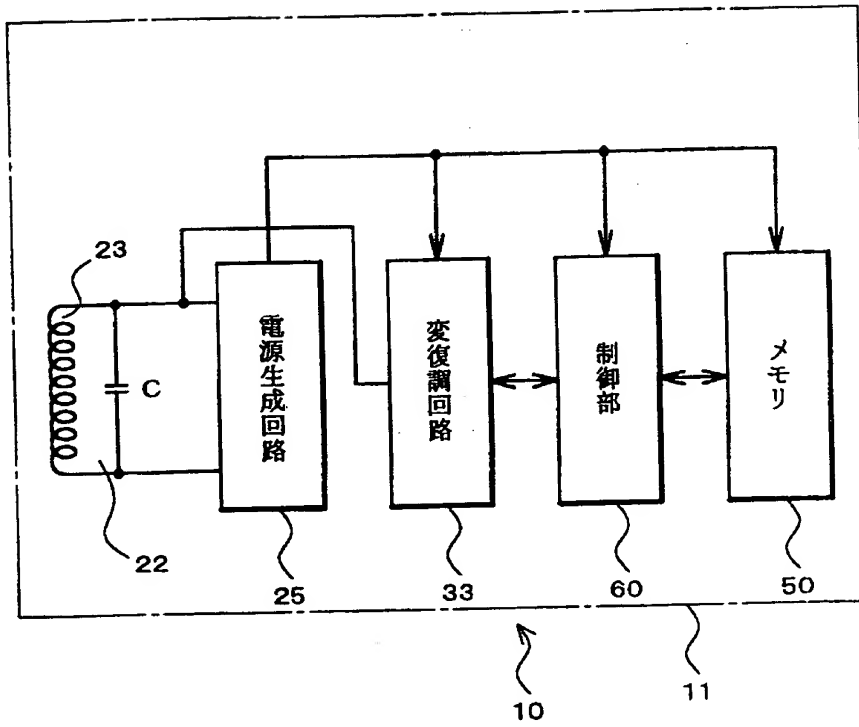
出願人代理人 弁理士 眞島宏明

【書類名】 図面

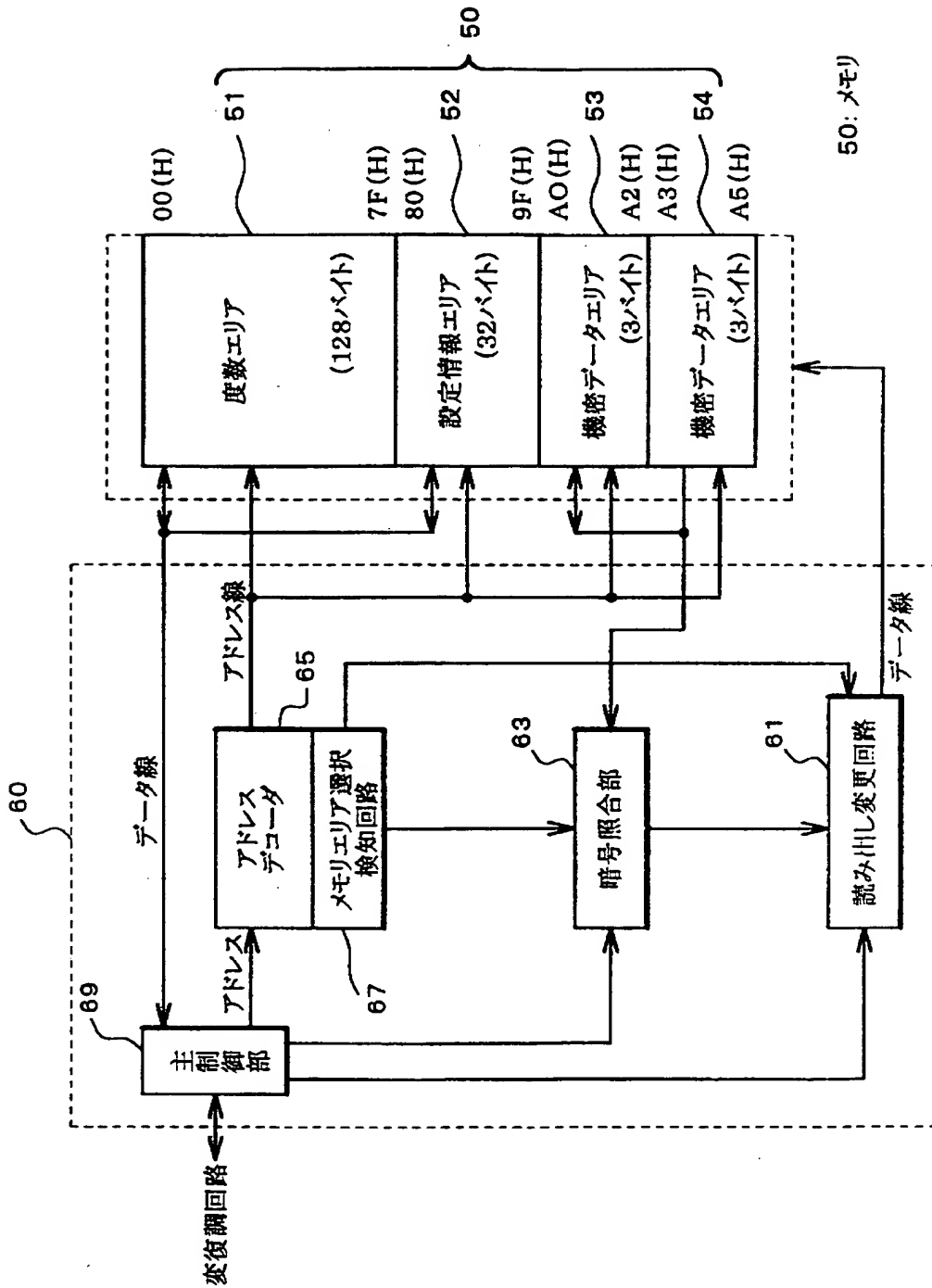
【図 1】



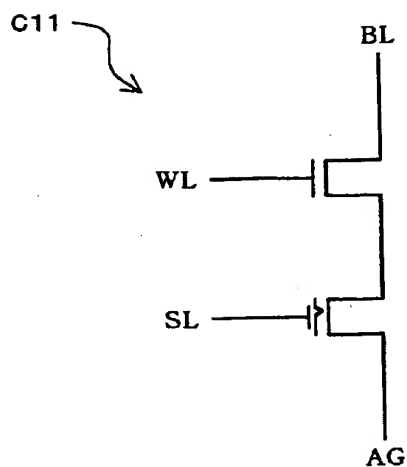
【図2】



【図 3】



【図4】

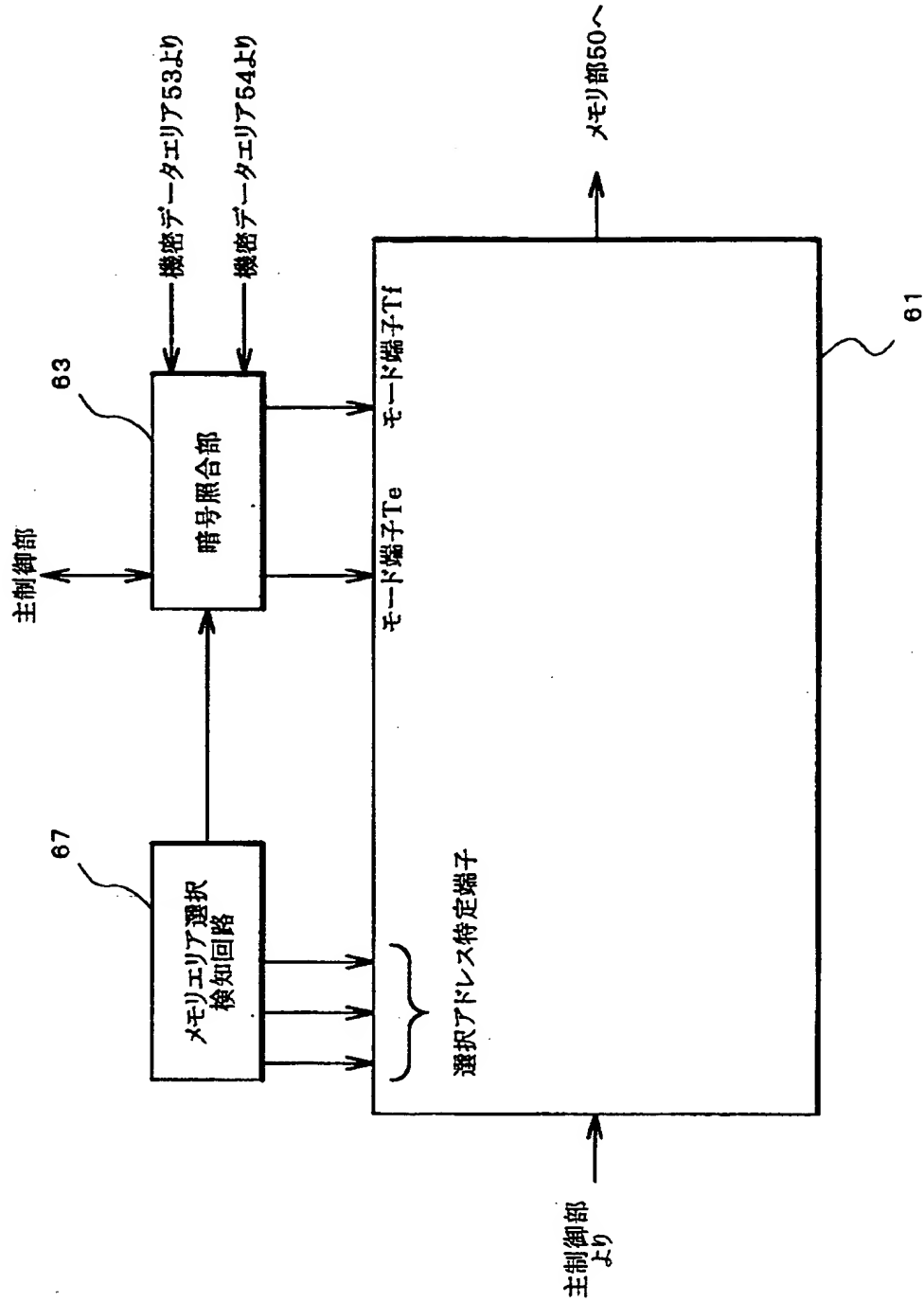


【図5】

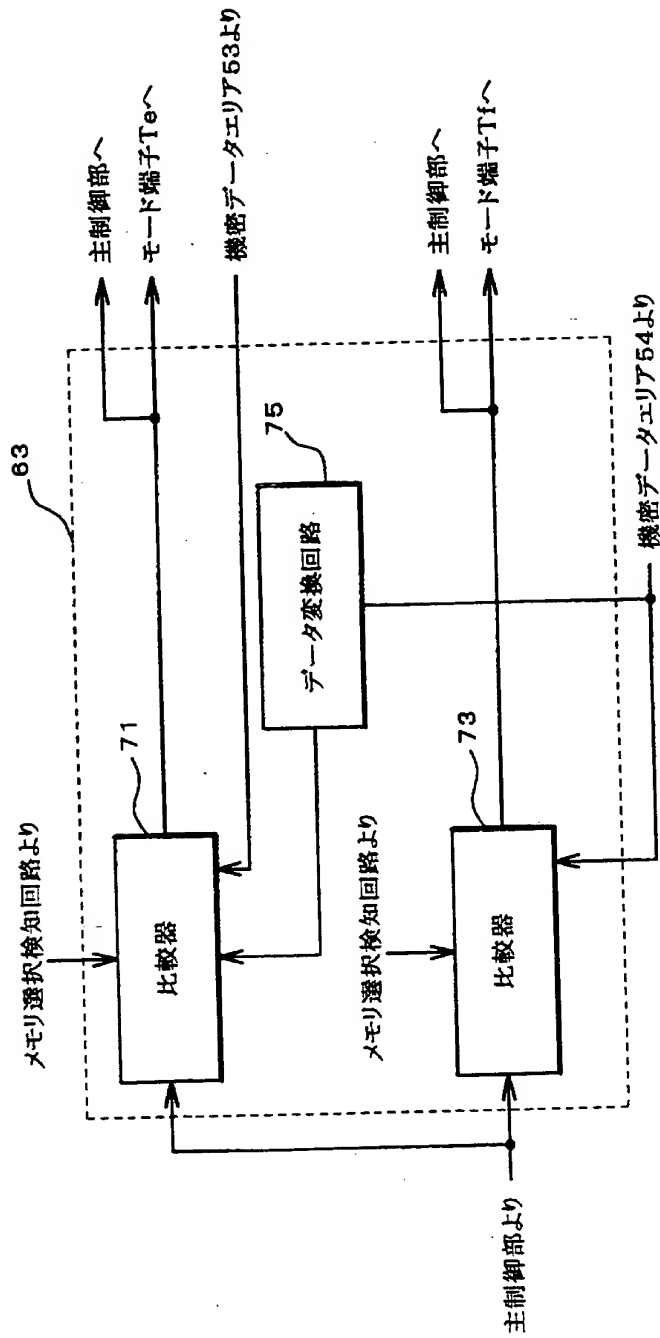
| | BL | SL | WL | AG |
|------|-------|-----|-----|------------------|
| 読み出し | データ出力 | 5V | 5V | 0V |
| 書き込み | 20V | 0V | 20V | open |
| 消去 | 0V | 20V | 20V | open or 0V |

データ変更 { 書き込み:「1」→「0」に書き換える
消去:「0」→「1」に書き換える

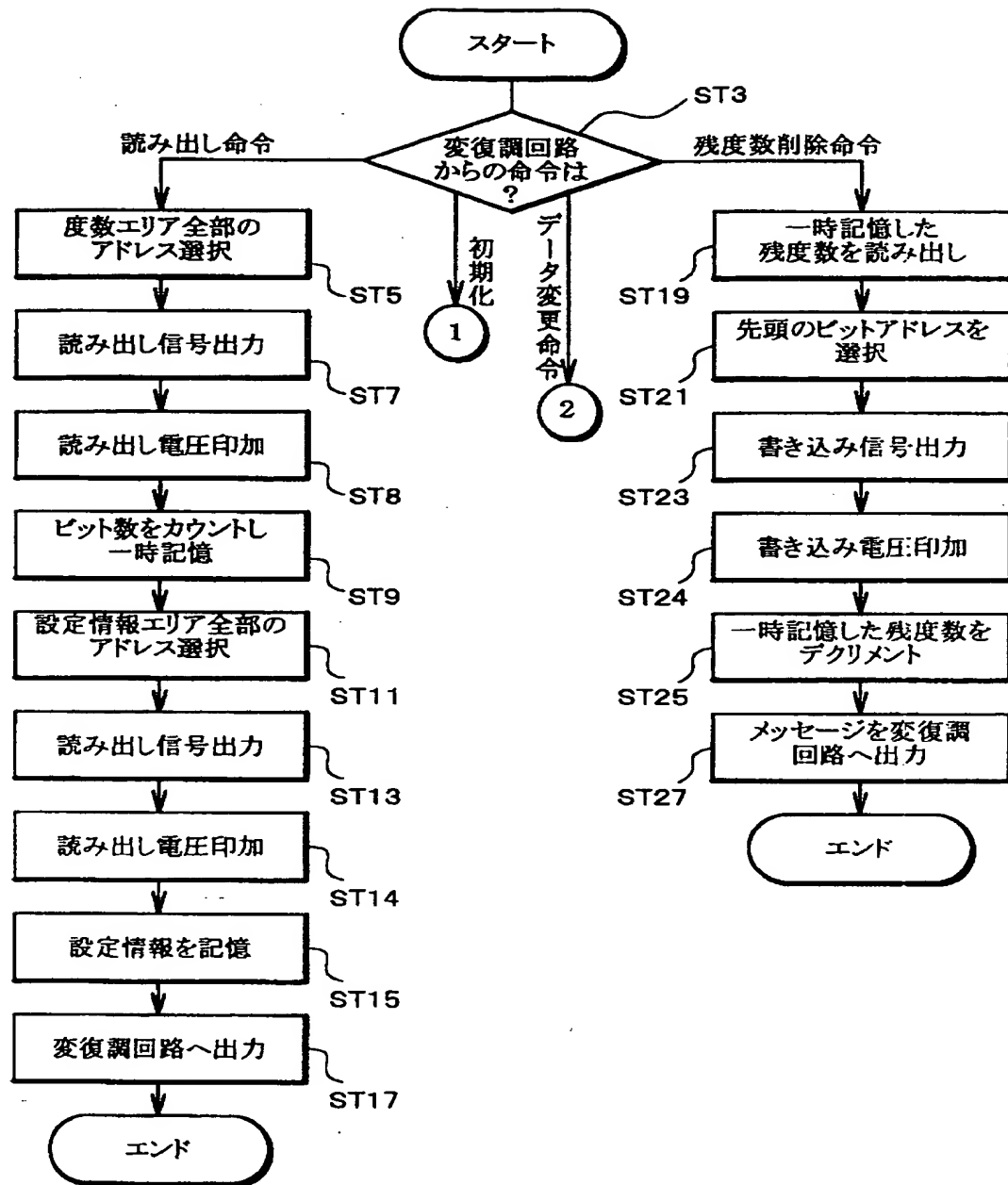
【図6】



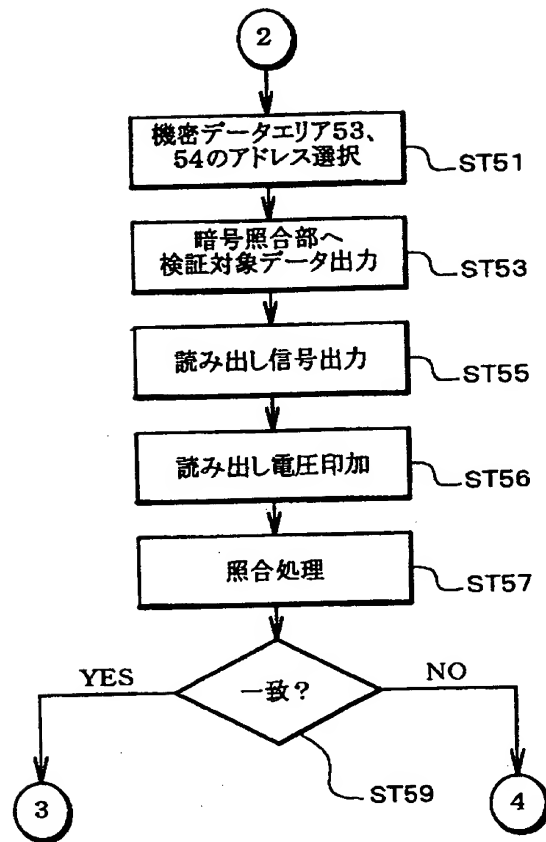
【図7】



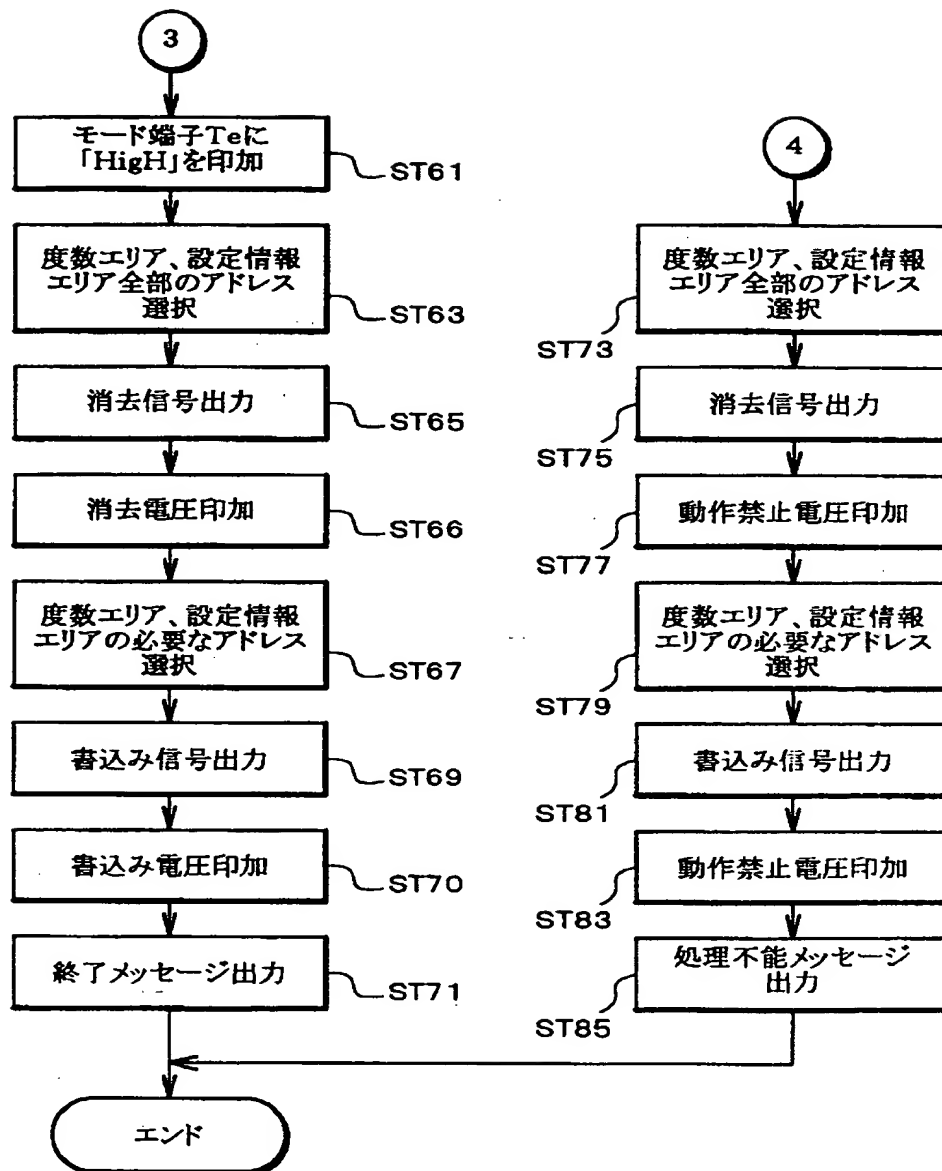
【図8】



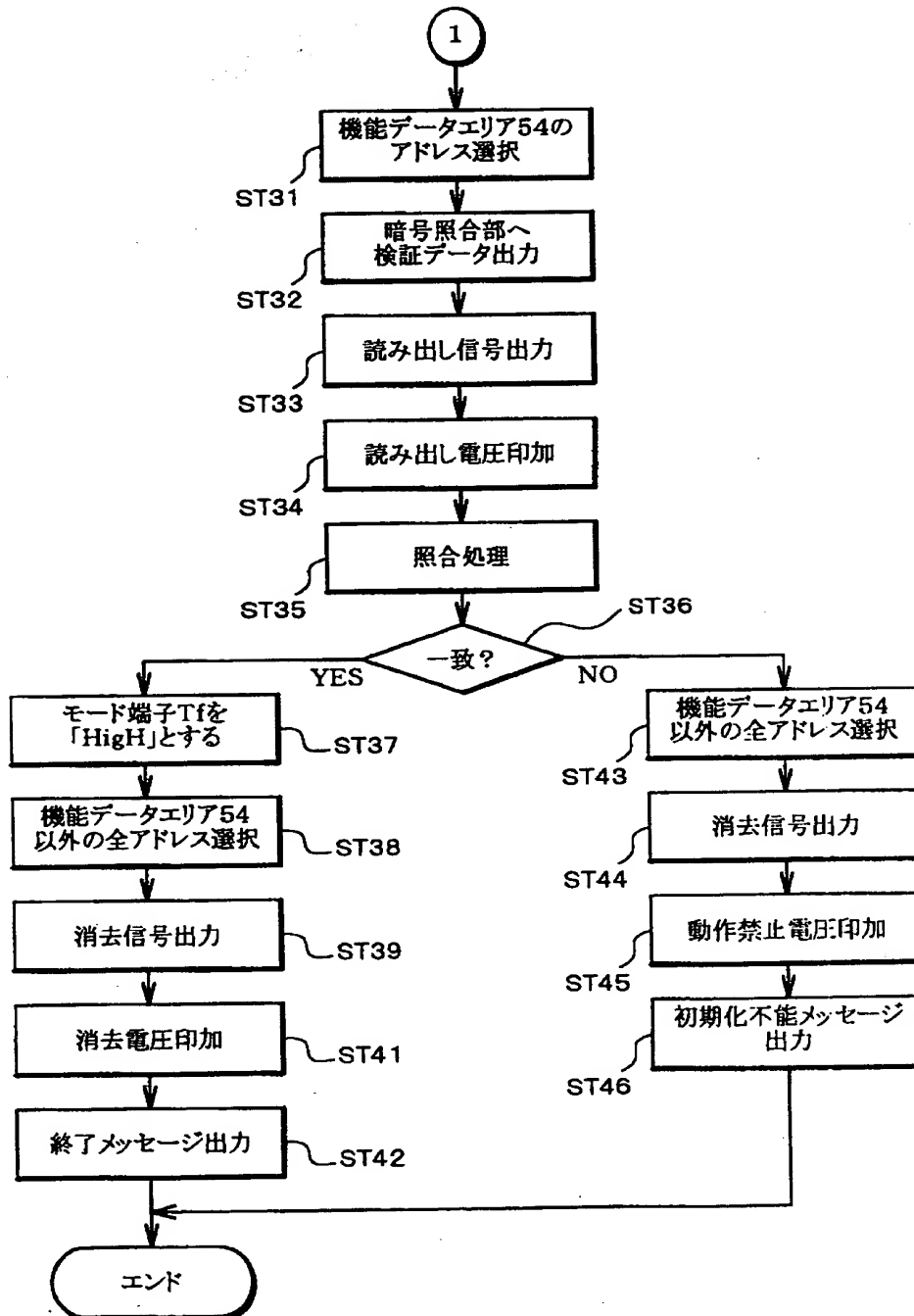
【図9】



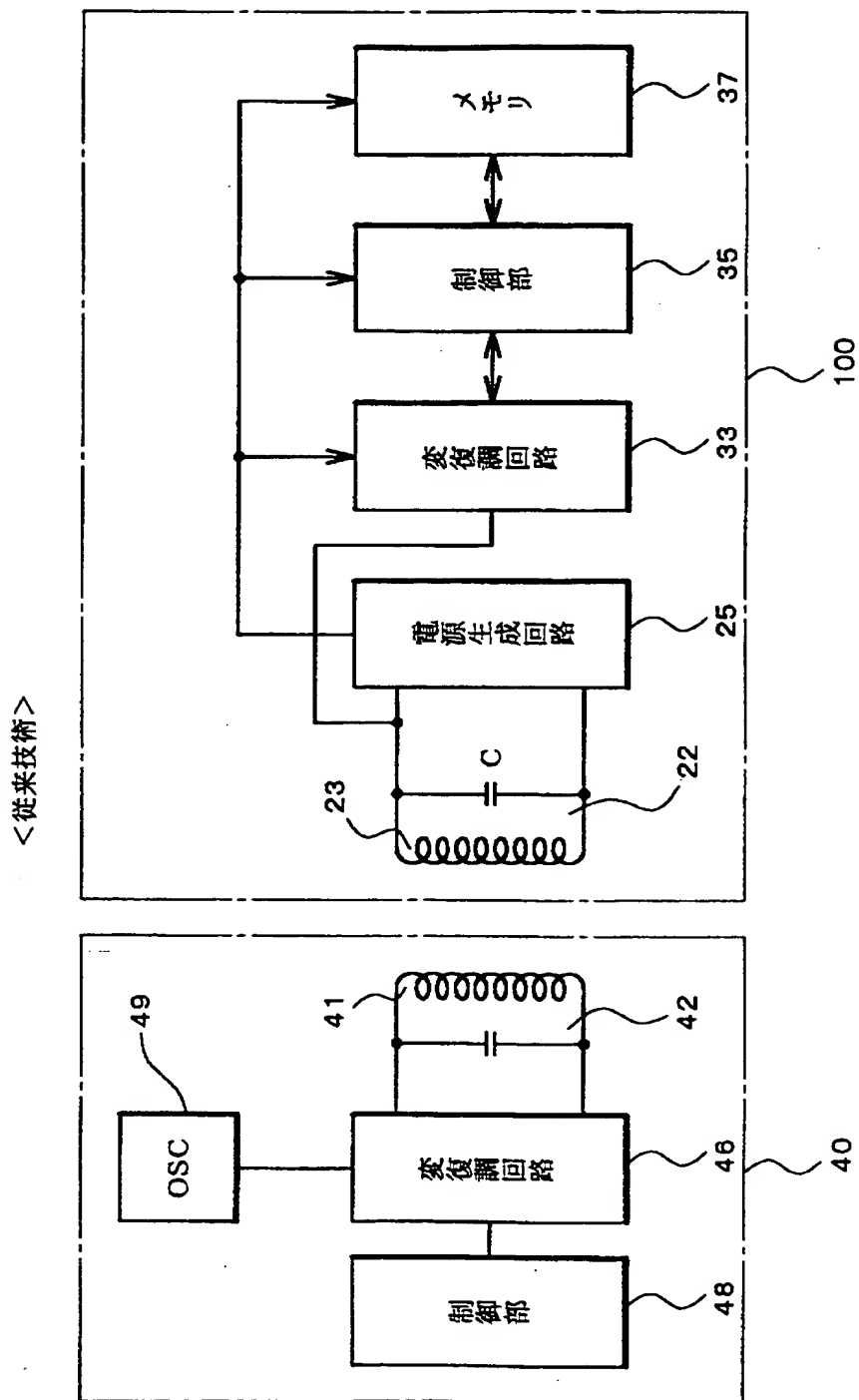
【図10】



【図11】



【図12】



【書類名】 要約書

【要約】

【課題】 変造が困難なＩＣカードを提供する。

【解決手段】 度数記憶手段３は、データ保持部を度数個数分有する。度数追加書換え用情報記憶手段１３は、度数追加書換え用情報を記憶する。照合手段１１は、与えられた情報と前記度数追加書換え用情報とを照合する。度数変更手段７は、前記各データ保持部を前記書込み状態から前記非書込状態に変更可能なだけでなく、さらに、照合手段１１の照合結果に基づいて、前記各データ保持部を前記非書込み状態から前記書込状態にも変更できる。度数変更手段７は、度数記憶部材の外部から与えられた度数変更命令に基づいて、前記各データ保持部に書込データを保持する書込み状態から書込データを保持しない非書込状態にだけ変更できる。

【選択図】 図１

【書類名】 職権訂正データ
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】 000116024

【住所又は居所】 京都府京都市右京区西院溝崎町2-1番地

【氏名又は名称】 ローム株式会社

【代理人】 申請人

【識別番号】 100092956

【住所又は居所】 大阪府吹田市江坂町1丁目2-3番20号 第二水川
ビル 古谷国際特許事務所

【氏名又は名称】 古谷 栄男

【選任した代理人】

【識別番号】 100101018

【住所又は居所】 大阪府吹田市江坂町1丁目2-3番20号 第二水川
ビル 古谷国際特許事務所

【氏名又は名称】 松下 正

【選任した代理人】

【識別番号】 100101546

【住所又は居所】 大阪府吹田市江坂町1丁目2-3番20号 第二水川
ビル 古谷国際特許事務所

【氏名又は名称】 眞島 宏明

出 願 人 履 歴 情 報

識別番号 [000116024]

1. 変更年月日 1990年 8月22日
[変更理由] 新規登録
住 所 京都府京都市右京区西院溝崎町21番地
氏 名 ローム株式会社